CLAIMS

What is claimed is:

1. A method for an authentication process within a distributed data processing system, the method comprising:

receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

forwarding the authentication data to a controlled resource.

2. The method of claim 1 wherein the controlled resource is a legacy application.

3. The method of claim 1 wherein the authentication data comprises a user identity and a password.

4. The method of claim 1 further comprising:

authenticating the client for access to the controlled resource based on the authentication data.

5. The method of claim 1, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the host.

6. The method of claim 1 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

7. The method of claim 1 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

8. A method for generating a digital certificate, the method comprising:

receiving, at an attribute-certificate-issuing authority, a request for an attribute certificate from a client;

generating the attribute certificate in response to the received request for an attribute certificate, wherein the attribute certificate comprises encrypted authentication data that was generated by encrypting authentication data for a controlled resource at a host with a public key associated with the host; and

sending the generated attribute certificate to the client.

9. The method of claim 8 wherein the controlled resource is a legacy application.

10. A method for obtaining a digital certificate, the method comprising:

retrieving a public key certificate associated with a host within a distributed data processing system;

extracting a public key associated with the host from the public key certificate;

encrypting with the public key authentication data for a controlled resource at the host;

generating a request for an attribute certificate;

storing the encrypted authentication data within the request for the attribute certificate;

sending the request for the attribute certificate to an attribute-certificate-issuing authority; and

receiving an attribute certificate from the attribute-certificate-issuing authority, wherein the attribute certificate comprises the encrypted authentication data.

11. The method of claim 10 wherein the controlled resource is a legacy application.

12. A data structure representing an attribute certificate for use in a data processing system, the data structure comprising:

an issuer name;

a signature;

a holder name;

an attribute containing encrypted authentication data that was generated by encrypting authentication data for a controlled resource at a host with a public key associated with the host.

13. The data structure of claim 12 wherein the controlled resource is a legacy application.

14. An apparatus for performing an authentication process within a distributed data processing system, the apparatus comprising:

receiving means for receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting means for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

decrypting means for decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

forwarding means for forwarding the authentication data to a controlled resource.

15. The apparatus of claim 14 wherein the controlled resource is a legacy application.

16. The apparatus of claim 14 wherein the authentication data comprises a user identity and a password.

17. The apparatus of claim 14 further comprising:

authenticating means for authenticating the client for access to the controlled resource based on the authentication data.

18. The apparatus of claim 14, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the apparatus further comprising:

first parsing means for parsing the authentication data to retrieve a specific set of authentication data for the host.

19. The apparatus of claim 14 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the apparatus further comprising:

second parsing means for parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

20. The apparatus of claim 14 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

21. An apparatus for generating a digital certificate, the apparatus comprising:

receiving means for receiving, at an attribute-certificate-issuing authority, a request for an attribute certificate from a client;

generating means for generating the attribute certificate in response to the received request for an attribute certificate, wherein the attribute certificate comprises encrypted authentication data that was generated by encrypting authentication data for a controlled resource at a host with a public key associated with the host; and

sending means for sending the generated attribute certificate to the client.

22. The apparatus of claim 21 wherein the controlled resource is a legacy application.

23. An apparatus for obtaining a digital certificate, the apparatus comprising:

retrieving means for retrieving a public key certificate associated with a host within a distributed data processing system;

extracting means for extracting a public key associated with the host from the public key certificate;

encrypting means for encrypting with the public key authentication data for a controlled resource at the host;

generating means for generating a request for an attribute certificate;

storing means for storing the encrypted authentication data within the request for the attribute certificate;

sending means for sending the request for the attribute certificate to an attribute-certificate-issuing authority; and

receiving means for receiving an attribute certificate from the attribute-certificate-issuing authority, wherein the attribute certificate comprises the encrypted authentication data.

24. The apparatus of claim 23 wherein the controlled resource is a legacy application.

25. A computer program product in a computer readable medium for use in a distributed data processing system for performing an authentication process, the computer program product comprising:

instructions for receiving an attribute certificate from a client at a host within the distributed data processing system;

instructions for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

instructions for decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

instructions for forwarding the authentication data to a controlled resource.

26. The computer program product of claim 25 wherein the controlled resource is a legacy application.

27. The computer program product of claim 25 wherein the authentication data comprises a user identity and a password.

28. The computer program product of claim 25 further comprising:

instructions for authenticating the client for access to the controlled resource based on the authentication data.

29. The computer program product of claim 25, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the computer program product further comprising:

instructions for parsing the authentication data to retrieve a specific set of authentication data for the host.

30. The computer program product of claim 25 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the computer program product further comprising:

instructions for parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

31. The computer program product of claim 25 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

32. A computer program product in a computer readable medium for use in a data processing system for generating a digital certificate, the computer program product comprising:

instructions for receiving, at an attribute-certificate-issuing authority, a request for an attribute certificate from a client;

instructions for generating the attribute certificate in response to the received request for an attribute certificate, wherein the attribute certificate comprises encrypted authentication data that was generated by encrypting authentication data for a controlled resource at a host with a public key associated with the host; and

instructions for sending the generated attribute certificate to the client.

33. The computer program product of claim 32 wherein the controlled resource is a legacy application.

34. A computer program product in a computer readable medium for use in a data processing system for obtaining a digital certificate, the computer program product comprising:

instructions for retrieving a public key certificate associated with a host within a distributed data processing system;

instructions for extracting a public key associated with the host from the public key certificate;

instructions for encrypting with the public key authentication data for a controlled resource at the host;

instructions for generating a request for an attribute certificate;

instructions for storing the encrypted authentication data within the request for the attribute certificate;

instructions for sending the request for the attribute certificate to an attribute-certificate-issuing authority; and

instructions for receiving an attribute certificate from the attribute-certificate-issuing authority, wherein the attribute certificate comprises the encrypted authentication data.

35. The computer program product of claim 34 wherein the controlled resource is a legacy application.